REMARKS

The new rejection of claims 26-33 and 42 under 35 USC §103(a) in view of U.S. Patent Publication No. 2002/012478 (Kocher) and U.S. Patent No. 6,337,909 (Vanstone) is respectfully traversed on the grounds that the Kocher publication and the Vanstone patent, whether considered individually or in any reasonable combination, fail to disclose or suggest the claimed combination of:

- falsifying secret input data by combination with auxiliary data before the execution of one or more operations;
- combining the output data determined by execution of the one or more operations with an auxiliary function value in order to compensate for the falsification of the input data; and
- the auxiliary function value having been previously determined by the execution of the one or more operations with the auxiliary data as input data in safe surroundings and stored along with the auxiliary data.

The Kocher publication discloses the first two steps, but not in combination with **pre-determination in safe surroundings** and **storage** of the auxiliary function value and auxiliary data, as claimed. Instead, Kocher discloses that the auxiliary data and auxiliary function value are computed **while** computing the permutation of the input data. As a result, the auxiliary function value and data are vulnerable to inspection by an attacker. The Vanstone patent does not make up for the failure of the Kocher publication to disclose implementation of the first two steps of the claimed method using a **previously determined** auxiliary function value, since the Vanstone patent does not disclose any sort of input data falsification with auxiliary data or compensating auxiliary function value, and therefore could not have suggested that the auxiliary function value should be previously determined and stored along with the auxiliary data, as claimed.

It appears from the Official Action that the Examiner has interpreted the value γ disclosed in the Vanstone patent as corresponding to the claimed auxiliary function value, and therefore concluded that since γ is precomputed and stored, that it would have been obvious to similarly precompute and store the auxiliary function value of Kocher. However, γ as disclosed in the

Vanstone patent has nothing to do with an auxiliary function value of the type claimed. To the contrary, γ is a computationally intensive component of a secret key α^k. The secret value γ of Vanstone is never applied to some input value in order to compensate for some operation performed on that input value by some kind of "auxiliary data." The fact that Vanstone pre-computes and stores a component of a secret key would not have suggested to one of ordinary skill in the art that Kocher's auxiliary function value should be pre-computed in a secure environment.

Whereas the Kocher publication concerns the same problem as the present invention, namely algorithm falsification to prevent compromise of secret input data upon intercepting signals generated during processing of the data, the Vanstone patent concerns a very different problem that is not obviously applicable to the claimed invention or to the method of Kocher. Vanstone instead is directed to a method of generating session parameters for use with public key protocols, as explained in col. 1, lines 12-14. In one embodiment of a public key encryption system, an integer k is used as a private key and is maintained secret, and a corresponding public key is obtained by exponentiating a group generator α with the integer k to provide a public key in the form α^k. As a result, the value of the integer k cannot be derived even though the value of α^k is known, as explained in col. 2, lines 27-32. This leads to the problem that, because the system is only secure if integer k is a relatively large number, the computation of α^k is computationally expensive. The Vanstone patent solves this problem selecting integers with low Hamming weights, and mathematically combining the result with secure value γ, which may be precomputed and stored. Basically, the computationally intensive part of the secret value calculation is carried out beforehand, and the computationally less expensive part of the secret value calculation can more easily be carried out as necessary to generate the session key.

In other words, **Vanstone teaches the principle of calculating the computationally intensive part of a secret "session key" beforehand (pre-computing and storing) in order to simplify the session key calculation at the time the session key is generated.** Vanstone teachings nothing about pre-computing and/or storing auxiliary function values used to compensate for data falsification. The Applicant is not claiming the general principle of pre-

computing secret values in a secure environment, but rather claims pre-computing, in a secure environment, a particular type of data used to compensate for falsification of secret data. The value pre-computed by the present invention, unlike a component of a secret key, has not previously been considered to be particularly secret, as evidenced by the fact that Kocher does not attempt to prestore the compensating value.

Not only does Vanstone concern a different problem than that faced by Kocher and the claimed invention, but the Vanstone patent uses the term "secure" in a different sense compared to the present invention. It is the aim of Vanstone to compute a computationally secure public key, that is, a key that cannot be broken by known computational attacks even though the attacker is able to read the public key on some communication channel. It is not objective of Vanstone to protect the system on which the computation of the session parameters is performed against external monitoring techniques that attack the system itself. No measures are, for example, disclosed by Vanstone to prevent an attacker from spying out the secret key k by monitoring the computation $k = k' + i$ that is used to store i securely. Furthermore, no means are provided to protect k or k' during the determination of k' and the computation of k.

Finally, it is respectfully noted that it is not at all obvious that the motivation for the combination set forth by the Examiner, namely pre-storing to achieve faster computation (which is the reason that Vanstone uses γ), is even applicable to the method of Kocher, *i.e.*, that pre-computing and storing the auxiliary values would have resulted in faster computation. From the description of the source code in paragraph [0068] of the Kocher publication, it does not appear that there would be any performance gain from reading the random values temp [i] and dataOut [i] in the first "for"-loop of Kocher and the random bits b in the third "for"-loop of Kocher from a disc where they were pre-computed and stored, rather than generating them using some optimized library function such as trueRandom() as taught by Kocher. Vanstone pre-computes because of the large numbers that must be manipulated to generate γ, whereas there is no reason to believe that Kocher's preferred number generator is slower than retrieving pre-computed values from storage.

In summary, Kocher teaches falsifying secret input data by combination with auxiliary data before the execution of one or more operations *and* combining the output data determined by execution of the one or more operations with an auxiliary function value in order to compensate for the falsification of the input data; but not the feature in which the auxiliary function value has been previously determined by the execution of the one or more operations with the auxiliary data as input data in safe surroundings and stored along with the auxiliary data. Vanstone teaches that a computationally intensive component of a secret key may be pre-computed and stored, so as to make it easier to generate the key when needed, but teaches nothing that would suggest pre-computing and storing the auxiliary values used by Kocher, which are not pre-computed and stored (as explained in more detail in the previous response). Furthermore, Vanstone does not even teach secure storage within the meaning of the invention, since the data used by Vanstone is actually exposed to interception of the type with which the present invention is concerned. Therefore, it is respectfully submitted that one of ordinary skill in the art would not have found it obvious to apply the teachings of Vanstone to the modify the method of Kocher, as claimed, and even if the respective teachings were to have someone been combined, the claimed invention would not have resulted. Withdrawal of the rejection of claims 26-33 and 42 is accordingly requested.

Having thus overcome the sole rejection made in the Official Action, expedited passage of the application to issue is requested.

Respectfully submitted,

BACON & THOMAS, PLLC

Date: April 8, 2008

By: BENJAMIN E. URCIA
Registration No. 33,805

Serial Number 09/700,656

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314

Telephone: (703) 683-0500